PROTECTION OF PERSONAL INFORMATION OPERATING POLICIES AND PROCEDURES

BRADSHAW LE ROUX CONSULTING

Address : 2 Inkonka Road, Kloof, 3610

Owner : Lesa Bradshaw

Email : Lesa@bradshawleroux.co.za

Tel : +27 31 765 2547

Introduction

We are committed to compliance with The Protection of Personal Information (POPI) Act which requires us to:

1. Sufficiently inform candidates/applicants, hereafter referred to as candidates, how we intend using their information.

2. Protect our Information assets from threats, whether internal or external, deliberate or accidental, to ensure business continuation, minimise business damage and maximise business opportunities.

This policy establishes general standards for the protection of personal information within our organisation and provides principles regarding the right of individuals to privacy and to reasonable safeguarding of their personal information.

The Information Officer, (Lesa Bradshaw), is responsible for:

- The development and upkeep of this policy.
- Ensuring this policy is supported by appropriate documentation.
- Ensuring that documentation is relevant and kept up to date.
- Ensuring this policy and subsequent updates are communicated to relevant managers, representatives, staff and associates, where applicable.

All employees, subsidiaries, business units, departments and individuals directly associated with us are responsible for adhering to this policy and for reporting any security breaches or incidents to the Information Officer.

Any Service Provider responsible for providing and managing information technology must adhere to the same information security principles contained in this policy to ensure security measures are in place in respect of processing of personal information.

Policy Principles

Principle 1: Accountability

- We must take reasonable steps to ensure that personal information obtained from candidates is stored safely and securely.
- This includes CV's, Resumes, References, Qualifications, Integrity Checks and any other personal information that may be obtained for the purpose of candidate representation.

Principle 2: Processing Limitation

We will collect personal information directly from candidates.

- Once in our possession we will only process or release candidate information with their consent, except where we are required to do so by law. In the latter case we will always inform the candidate.

Principle 3: Specific Purpose

- We collect personal information from candidates to enable us to represent them to our clients for the purpose of recruitment.

Principle 4: Limitation on Further Processing

- Personal information may not be processed further in a way that is incompatible with the purpose for which the information was collected initially. We collect personal information for recruitment, and it will only be used for that purpose.

Principle 5: Information Quality

- We are responsible for ensuring that candidate information is complete, up to date and accurate before we use it. This means that it may be necessary to request candidates, from time to time, to update their information and confirm that it is still relevant. If we are unable to reach a candidate for this purpose their information will be deleted from our records.

Principle 6: Transparency/Openness

- Where personal information is collected from a source other than directly from a candidate (EG social media, portals) we are responsible for ensuring that the candidate is aware:
    - That their information is being collected.
    - Who is collecting their information by giving them our details.
    - Of the specific reason you are collecting their information.

Principle 7: Security Safeguards

- We will ensure technical and organizational measures to secure the integrity of personal information, and guard against the risk of loss, damage or destruction thereof. Personal information must also be protected against any unauthorized or unlawful access or processing. We are committed to ensuring that information is only used for legitimate purposes with candidate consent and only by authorized employees of our agency.

Principle 8: Participation of Individuals

- Candidates are entitled to know particulars of their personal information held by us, as well as the identity of any authorized employees of our agency that had access thereto. They are also entitled to correct any information held by us.

Operational Considerations

Monitoring

The Board/Management and Information Officer are responsible for administering and overseeing the implementation of this policy and, as applicable, supporting guidelines, standard operating procedures, notices, consents and appropriate related documents and processes. All employees, subsidiaries, business units, departments and individuals directly associated with us are to be trained, according to their functions, in the regulatory requirements, policies and guidelines that govern the protection of personal information. We will conduct periodic reviews and audits, where appropriate, to ensure compliance with this policy and guidelines.

Operating controls

We shall establish appropriate standard operating procedures that are consistent with this policy and regulatory requirements. This will include:

- Allocation of information security responsibilities.
- Incident reporting and management.
- User ID addition or removal.

- Information security training and education.
- Data backup.

Policy Compliance

Any breach/es of this policy may result in disciplinary action and possible termination of employment.